Veri İşleyen Sözleşmesi (DPA)

1. Taraflar

İşbu Veri İşleyen Sözleşmesi ve Gizlilik Taahhütnamesi ("Sözleşme"), **Webhosting Bilişim Teknolojileri A.Ş.** (bundan sonra **ProMail** veya **Veri İşleyen** olarak anılacaktır) ile **www.promail.com.tr** ("Site") üzerinden kurumsal e-posta barındırma, arşivleme, bulut ve sunucu altyapı hizmeti satın alan gerçek veya tüzel kişi ("Müşteri" veya "Veri Sorumlusu") arasında standart ek sözleşme olarak akdedilmiştir:

1. Veri Sorumlusu (Müşteri):
Webhosting Bilişim Teknolojileri A.Ş. (bundan sonra **ProMail** olarak anılacaktır) ile **www.promail.com.tr** ("Site") üzerinden kurumsal e-posta barındırma, e-posta arşivleme, sunucu veya bulut altyapı hizmeti satın alan ve müşteri panelinde kayıtlı bulunan gerçek veya tüzel kişi ("Müşteri").

2. Veri İşleyen (Hizmet Sağlayıcı — ProMail):
Ticari Unvan: Webhosting Bilişim Teknolojileri A.Ş.
Vergi Dairesi / No: Sultanbeyli / 8000539679 | **MERSİS No:** 0800 0539 6790 0018
Adres: Meclis Mah. Derviş Sok. Fuat Özal Plaza No:38/1 Sancaktepe / İstanbul
İletişim / E-Posta: destek@promail.com.tr | **Tel:** +90 (216) 606 55 27

Taraflar işbu Sözleşme'de münferiden "Taraf", müştereken "Taraflar" olarak anılacaktır.

2. Tanımlar ve Hizmet Modeli

Bu Sözleşme'de geçen;

- **Kanun (KVKK):** 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
- **Kurul:** Kişisel Verileri Koruma Kurulu'nu,
- **Kişisel Veri, Özel Nitelikli Kişisel Veri, İlgili Kişi, Veri Sorumlusu ve Veri İşleyen:** Kanun'da belirtilen yasal tanımları,
- **Ana Sözleşme:** Taraflar arasında kurulan Hizmet Sözleşmesi, Kurumsal E-Posta Barındırma Sözleşmesi veya sipariş özeti niteliğindeki temel hizmet ilişkisini ve eklerini,
- **Hizmet Modeli:** Veri İşleyen tarafından sunulan ve sipariş esnasında belirlenen; kurumsal e-posta servis omurgası (SmarterMail / PMG), paylaşımlı barındırma veya sunucu altyapısı sağlama modelini ifade eder.

3. Sözleşmenin Konusu ve İşleme Faaliyetinin Kapsamı

- **3.1.** İşbu Sözleşme, Veri Sorumlusu'nun Veri İşleyen altyapısında barındırdığı kurumsal e-posta hesapları, ekler, adres defterleri, takvim kayıtları ve diğer kişisel verilerin Kanun'un 12. maddesine uygun olarak muhafazasına ilişkin tarafların hak, yetki ve yükümlülüklerini düzenler.

- **3.2.** Veri İşleyen'in veri işleme faaliyeti; e-posta sunucuları, spam/antivirüs ağ geçitleri (Mail Gateway) ve depolama kaynaklarının çalışır durumda tutulması, iletilerin alıcıya teslimi, yedeklenmesi ve altyapı sürekliliği için zorunlu olan otomatik teknik işlemlerle sınırlıdır.
- **3.3.** Veri İşleyen; tahsis edilen e-posta kutularının veya sunucuların içerisindeki verilere beşeri olarak erişmez, yazışmaların içeriğini denetlemez, kopyalamaz ve Veri Sorumlusu'nun açık yazılı/destek talebi talimatı veya yasal zorunluluklar haricinde verilere hiçbir surette müdahale etmez.

4. Güvenlik Tedbirleri ve Paylaşımlı Sorumluluk Modeli

Taraflar, kurumsal e-posta ve bulut barındırma hizmetinin teknik doğası gereği güvenlik sorumluluklarının **Paylaşımlı Sorumluluk Modeli (Shared Responsibility Model)** çerçevesinde aşağıdaki gibi paylaşıldığını kabul ve taahhüt ederler:

- **4.1. Veri İşleyen'in Sorumluluk Alanı (Altyapı ve Servis Omurgası Güvenliği):** Veri İşleyen; veri merkezine fiziksel erişim güvenliği, enerji ve iklimlendirme yedekliliği, sanallaştırma (hipervizör) ve posta sunucusu işletim sistemi katmanlarının güvenliği, ağ geçidi seviyesinde (PMG) yapay zeka destekli anti-spam/antivirüs filtrelemesi, şifreli iletişim protokollerinin (SSL/TLS) sunulması, izole günlük yedekleme ve ağ seviyesindeki (L3/L4) genel DDoS filtreleme tedbirlerini almakla yükümlüdür.
- **4.2. Veri Sorumlusu'nun Sorumluluk Alanı (Hesap ve Uç Nokta Güvenliği):** E-posta kullanıcı parolalarının karmaşıklığı ve gizliliği, iki aşamalı doğrulama (2FA) özelliklerinin aktif edilmesi, müşteri yönetim paneli yetkileri ve uç nokta (bilgisayar/mobil cihaz) güvenliği münhasıran Veri Sorumlusu'nun sorumluluğundadır.
  - **a)** Müşteri'nin veya kullanıcılarının kendi cihazlarına bulaşabilecek zararlı yazılımlar (trojan, keylogger, casus yazılım vb.),
  - **b)** Oltalama (phishing), sosyal mühendislik veya zayıf/tahmin edilebilir parola tercihleri neticesinde e-posta veya panel erişim bilgilerinin yetkisiz üçüncü kişilerin eline geçmesi,
  - **c)** Yönetilmeyen (unmanaged) sanal sunucu hizmetlerinde işletim sistemi, güvenlik duvarı ve uygulama katmanı açıkları,

  doğrudan Veri Sorumlusu'nun (Müşteri) kontrol ve sorumluluk alanında olup; bu yollarla gerçekleşen veri sızıntısı, hesap ele geçirme veya yetkisiz müdahalelerden Veri İşleyen hiçbir surette sorumlu tutulamaz.

5. Veri Konumu, Ağ Trafiği ve Alt Veri İşleyenler

- **5.1. %100 Yerli Veri Konumu:** ProMail kurumsal e-posta sunucuları, depolama alanları ve izole sistem yedekleri münhasıran **Türkiye Cumhuriyeti sınırları içerisindeki kurumsal veri merkezinde (İstanbul MARS Veri Merkezi)** barındırılır; posta kutusu verileri ve yedekleri yurt dışına aktarılmaz veya yurt dışındaki sunucularda depolanmaz.
- **5.2. Küresel E-Posta ve Ağ Trafiği İstisnası:** Elektronik posta protokolünün (SMTP) küresel yapısı gereği Veri Sorumlusu kullanıcılarının yurt dışındaki alıcılara gönderdiği veya yurt dışındaki göndericilerden aldığı e-postaların internet omurgası üzerinden iletilmesi ile siber saldırıların engellenmesi amacıyla yürütülen ağ seviyesindeki (L3/L4) DDoS filtreleme süreçleri Veri İşleyen tarafından yapılan bir yurt dışı veri aktarımı sayılmaz.

- **5.3. Alt Veri İşleyenler:** Veri İşleyen, hizmetin ifası için Türkiye'de yerleşik veri merkezi işletmecilerini, internet omurga operatörlerini ve siber güvenlik hizmet sağlayıcılarını alt veri işleyen olarak kullanmaya yetkilidir. Alt veri işleyenler işbu Sözleşme'dekilerle aynı düzeyde güvenlik ve gizlilik yükümlülüklerine tabidir.

6. Gizlilik Taahhütnamesi

- **6.1.** Veri İşleyen, işbu Sözleşme kapsamında sunulan hizmet vesilesiyle muttali olabileceği her türlü kişisel veriyi, ticari sırrı ve Veri Sorumlusu'na ait sistem bilgilerini süresiz olarak gizli tutacağını taahhüt eder.
- **6.2.** Veri İşleyen, personeline yalnızca görevlerinin gerektirdiği ölçüde altyapı erişimi tanır ve tüm personelinin süresiz gizlilik taahhüdü altında olmasını sağlar.
- **6.3.** Yetkili adli ve idari mercilerden gelebilecek yasal bilgi/erişim talepleri haricinde, Veri Sorumlusu'na ait hiçbir veri üçüncü kişilerle paylaşılamaz. İşbu gizlilik taahhüdü sözleşme sona erse dahi süresiz olarak yürürlükte kalır.

7. Güvenlik İhlallerinin Bildirimi

Veri İşleyen, kendi kontrolündeki fiziksel altyapı veya posta sunucusu katmanında doğrudan kişisel verileri etkileyebilecek doğrulanmış bir güvenlik ihlali tespit etmesi halinde; durumu teknik inceleme ve doğrulamanın tamamlanmasını müteakip **gecikmeksizin ve her hâlükârda en geç 72 (yetmiş iki) saat içinde** Veri Sorumlusu'na yazılı olarak bildirir. Veri Sorumlusu'nun kendi kullanıcılarının parola güvenliği ihlalleri veya uç nokta zararlı yazılımlarından kaynaklanan olaylar Veri İşleyen'in ihlal bildirim yükümlülüğü kapsamında değerlendirilmez.

8. Sorumluluğun Sınırlandırılması (Liability Cap)

- **8.1.** Taraflardan her biri, işbu Sözleşme'ye veya mevzuata aykırı kusurlu fiillerinden kaynaklanan zararlardan kendi kusuru oranında sorumludur.
- **8.2.** Tarafların kasıt veya ağır kusur halleri saklı kalmak kaydıyla; Veri İşleyen'in işbu Sözleşme'den, ifadan veya KVKK mevzuatından kaynaklanabilecek her türlü idari para cezası, tazminat ve rücu taleplerine karşı toplam mali sorumluluğu; Veri Sorumlusu tarafından ihlal veya talep tarihinden geriye dönük son 12 (on iki) ay içerisinde (hizmet süresi 12 aydan kısa ise hizmetin başladığı tarihten itibaren fiilen geçen süre boyunca) ilgili hizmet kapsamında Veri İşleyen'e **fiilen ve nakden ödenmiş olan toplam net hizmet bedeli ile sınırlıdır.** Dolaylı zararlar, kâr kaybı ve itibar kaybı tazminat kapsamı dışındadır.

9. Sözleşmenin Sona Ermesi, Verilerin Tahliyesi ve İmhası

- **9.1.** İşbu Sözleşme sipariş/onay tarihinde yürürlüğe girer ve Ana Sözleşme yürürlükte kaldığı sürece geçerlidir.
- **9.2.** Hizmetin sona ermesi veya vadesinde ödenmeyen faturalar nedeniyle durdurulması halinde, posta kutusu veya sunucu içerisindeki verilerin dışa aktarımı ve tahliyesi münhasıran Veri Sorumlusu'nun sorumluluğundadır. Veri Sorumlusu'na verilerini dışa aktarabilmesi adına **7 (yedi) takvim günü tahliye süresi** tanınır. Süre sonunda aktif depolama alanları ve son 14 günlük yedek periyodu tamamlandığında yedek kopyalar sistemden otomatik ve geri döndürülemez şekilde silinir.

- **9.3.** Veri Sorumlusu'nun talep etmesi halinde silme işleminin tamamlandığı e-posta yoluyla teyit edilir.

10. Uygulanacak Hukuk ve Yetkili Mahkeme

İşbu Sözleşme Türk hukukuna tabidir. Uyuşmazlıkların çözümünde **İstanbul Anadolu / Merkez (Çağlayan) Mahkemeleri ve İcra Daireleri** yetkilidir.

11. Yürürlük

11 (on bir) maddeden oluşan işbu Sözleşme; Müşteri'nin web sitesi üzerinden elektronik ortamda siparişi onaylaması, hizmetten yararlanmaya başlaması veya karşılıklı teyidi ile yürürlüğe girer ve Taraflar arasında bağlayıcı hüküm ifade eder.
